

1                   IN THE UNITED STATES DISTRICT COURT  
2                   FOR THE EASTERN DISTRICT OF VIRGINIA  
3                   Newport News Division

4                   -----  
5                   UNITED STATES OF AMERICA,                 )  
6    )  
7                   Plaintiff,                                      )  
8    )  
9                   v.    )    CRIMINAL CASE NO.  
10    )  
11    )  
12    )  
13    )  
14    )  
15    )  
16    )  
17    )  
18    )  
19    )  
20    )  
21    )  
22    )  
23    )  
24    )  
25    )

10    )  
11    )  
12    )  
13    )  
14    )  
15    )  
16    )  
17    )  
18    )  
19    )  
20    )  
21    )  
22    )  
23    )  
24    )  
25    )

TRANSCRIPT OF PROCEEDINGS

Norfolk, Virginia  
June 14, 2016

BEFORE: THE HONORABLE HENRY COKE MORGAN, JR.  
United States District Judge

APPEARANCES:

UNITED STATES ATTORNEY'S OFFICE  
By: Kaitlin C. Gratton  
Jay V. Prabhu  
Assistant United States Attorneys  
Counsel for the United States

FEDERAL PUBLIC DEFENDER'S OFFICE  
By: Andrew W. Grindrod  
Assistant Federal Public Defender  
Counsel for the Defendant

1	I N D E X			
2	ON BEHALF OF THE DEFENDANT:	Direct	Cross	Red.
3	D. Alfin	4	21	32
4				--
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

9	E X H I B I T S
10	
11	No. Page
12	(None)
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	

3 THE CLERK: Criminal Case No. 4:16cr16, the United  
4 States of America v. Edward Joseph Matish, III.

5 Ms. Gratton, Mr. Prabhu, are you ready to proceed  
6 for the government?

7 MS. GRATTON: The government is ready to proceed.

8 | Good afternoon, Your Honor.

9 THE COURT: Good afternoon.

10 THE CLERK: Mr. Grindrod, i

10 THE CLERK: Mr. Grindrod, is your client ready to  
11 proceed?

12 MR. GRINDROD: Mr. Matish is ready to proceed.

13 | Good afternoon, Your Honor.

14 THE COURT: All right. We're here on the  
15 defendant's discovery motion. Does either side have any  
16 evidence to present, or just argument?

17 MS. GRATTON: The government is prepared to present  
18 brief testimony from Agent Alfin in response to the most  
19 recently filed declaration, if the Court would find it  
20 helpful.

21 | THE COURT: Do you have any evidence?

22 MR. GRINDROD: Not that hasn't been already  
23 submitted, Your Honor.

24 THE COURT: By that you mean the declaration?

25 MR. GRINDROD: That's correct, Your Honor.

—D. Alfin - Direct—

1                   THE COURT: Okay. Well, do you have any evidence?

2                   MS. GRATTON: If the Court would permit, we would  
3 briefly call Agent Alfin to the stand.

4                   THE COURT: All right.

5                   (The clerk administered the oath.)

6                   DANIEL ALFIN, called as a witness, having been first  
7 duly sworn, testified as follows:

8                   DIRECT EXAMINATION

9 BY MS. GRATTON:

10 Q. Good afternoon. Can you please introduce yourself to the  
11 Court?

12 A. My name is Daniel Alfin. I am a Special Agent with the  
13 FBI. I am currently assigned to FBI Headquarters, Criminal  
14 Investigative Division, Violent Crimes Against Children  
15 Section, Major Case Coordination Unit, located in Lithicum,  
16 Maryland.

17 Q. And you're familiar with the case involving Edward  
18 Matish, III?

19 A. I am.

20 Q. And you've testified previously with respect to the  
21 motions to suppress the NIT warrant.

22 A. I have.

23 Q. You also submitted a witness declaration in response to  
24 the motion to compel discovery for which we are here today.

25 A. That's correct, I've submitted a declaration.

—D. Alfin - Direct—

1 Q. Have you reviewed the other declaration submitted by the  
2 defendant in support of his motion to compel?

3 A. I have.

4 Q. Including, most recently, the declaration submitted of  
5 Dr. Christopher Soghoian?

6 A. Yes, I have.

7 THE COURT: Dr. who, now? Oh, the most recent one?

8 MS. GRATTON: The most recent declaration.

9 THE COURT: Right.

10 BY MS. GRATTON:

11 Q. Before we move into that, can you briefly remind the  
12 Court -- the Court is obviously familiar with the network  
13 investigative technique, but the nature of the information  
14 collected by the operation of that technique in this case?

15 A. The information collected by the network investigative  
16 technique was a limited set of information originating from  
17 the computer of Mr. Matish. That information was authorized  
18 by a search warrant in the Eastern District of Virginia. The  
19 information that was collected was within the scope of that  
20 search warrant.

21 Additionally, all the information that was collected  
22 has been provided to defense for review or has been made  
23 available to defense for review.

24 Q. And that includes the MAC address?

25 A. Correct, it included the MAC address of the computer, the

—D. Alfin - Direct—

1 operating system version --

2 THE COURT: The what kind of address?

3 THE WITNESS: Your Honor, in order to connect to the  
4 Internet or any network, a computer has a network card in it.  
5 It could be a wireless network card, or it could be a  
6 hard-wired network card that you plug a cable into. All of  
7 these network cards, regardless of the type, have a MAC  
8 address.

9 THE COURT: A MAC address?

10 THE WITNESS: Yes, Your Honor. MAC is an acronym  
11 that stands for media address control.

12 THE COURT: Is that different than IP address?

13 THE WITNESS: Yes, Your Honor. A MAC address is  
14 unique and does not change. So you can look at the MAC  
15 address in the matter at hand from Mr. Matish's computer, and  
16 that MAC address is always the same. It is the one that was  
17 identified by the government. It was also the one that was  
18 seized by the government. A MAC address is hard-wired or  
19 burned into the card.

20 THE COURT: And the MAC address was among the  
21 information seized, in addition to the IP address?

22 THE WITNESS: Yes, Your Honor, also listed in the  
23 warrant attachment.

24 THE COURT: Okay.

25 BY MS. GRATTON:

—D. Alfin - Direct—

1 Q. And also the operating system?

2 A. Correct, the version of the operating system that was  
3 active on the computer, the name of the computer itself, and  
4 the user name that was currently logged in to the computer.

5 Q. And all of those items were listed in Attachment B of the  
6 search warrant?

7 A. Yes, in one of the attachments to the search warrant.

8 Q. Is there other information related to the user account on  
9 the Playpen Web site? As part of the investigation, was that  
10 information maintained?

11 A. Yes, during the course of the investigation the FBI  
12 monitored the activity on the Playpen Web site and captured  
13 the activity associated with each individual user on the  
14 Playpen Web site. In the matter at hand that involved  
15 information pertaining to the user account on the Playpen Web  
16 site named Broden. That information was collected by the  
17 government as it was monitoring the Web site. It was not  
18 collected as a function of the NIT.

19 Q. Are you familiar with the information --

20 THE COURT: Now, wait a minute. The information  
21 about the Broden account was obtained from the Web site --  
22 what Web site?

23 THE WITNESS: Your Honor, the FBI, for a limited  
24 period of time, operated the Playpen Web site.

25 THE COURT: Right.

—D. Alfin - Direct—

1                   THE WITNESS: Which is the Web site the defendant is  
2 accused of accessing. While we were operating the Web site  
3 we were also monitoring and recording every action that every  
4 user took on the Web site, so we were able to see for the  
5 matter at hand -- for the Broden account we can see every  
6 time the Broden account logged in, we can see where they went  
7 on the Web site, we can see what posts they accessed on the  
8 Web site, and we have a report that we've made available to  
9 defense so they can see every individual action, broken down  
10 by date and time, that the Broden user took on the Web site.

11                  THE COURT: But you didn't know who the Broden  
12 account was at that time. Is that right?

13                  THE WITNESS: Correct, Your Honor. That information  
14 was collected independent of the NIT.

15                  THE COURT: Before the NIT was --

16                  THE WITNESS: Both before, during, and after.

17                  THE COURT: Well, but you had -- you were able to  
18 see the activity of the Broden account without having to  
19 activate the NIT.

20                  THE WITNESS: That is correct.

21                  THE COURT: How did you do that?

22                  THE WITNESS: Because we had control of the Web  
23 site, we could see where all the users were going on the Web  
24 site. Even without being able to fully identify them, we  
25 could still see what the Broden --

—D. Alfin - Direct—

1                   THE COURT: So in order to find out who Broden was  
2 you had to employ the NIT. Is that correct?

3                   THE WITNESS: That's correct, Your Honor.

4                   THE COURT: Which you did.

5                   THE WITNESS: That's correct, Your Honor.

6                   THE COURT: Okay.

7 BY MS. GRATTON:

8 Q. Are you familiar with the information that has been  
9 disclosed in discovery or made available in this case?

10 A. I am.

11 Q. Can you briefly summarize that for the Court?

12 A. Several pieces of evidence have either been turned over  
13 to defense or made available for defense to review. One of  
14 those pieces of evidence is the activity that we monitored  
15 and collected on the Web site. That's the activity that  
16 shows when the Broden user account logged in to the Web site,  
17 where the Broden user account went to on the Web site, every  
18 post that the Broden user account accessed while the FBI was  
19 monitoring the Web site.

20                   In addition to that, we also have turned over to  
21 defense the source code for the NIT, for the network  
22 investigative technique, that collected the limited amount of  
23 information from Mr. Matish's computer. That source code has  
24 been turned over to the defense for review. The important  
25 thing about that source code is that it can be observed,

—D. Alfin - Direct—

1 analyzed, and it can be executed to confirm that it collects  
2 exactly what the FBI says it collects. And, additionally, it  
3 can be executed and viewed to confirm that the information  
4 that the FBI collected and made available in discovery did,  
5 in fact, originate from Mr. Matish's computer.

6 Q. And what would that process involve?

7 A. What we turned over is the source code for the NIT. And,  
8 so, Mr. Matish or a defense expert would take that code and  
9 compile it, which means just turning it into a program that  
10 you can run on a computer.

11 And, so, if I were the defense expert, if I was  
12 going to verify the address of the NIT, I would take that  
13 source code, I would compile it, and because Mr. Matish's  
14 computer is available for defense to review, they can  
15 actually execute the NIT on a copy of Mr. Matish's computer  
16 and confirm that it does exactly what the FBI says it does,  
17 no more than what the FBI says it does, and that the  
18 information that it collects is what was turned over in  
19 discovery and is true and accurate. They have everything  
20 that they need in order to complete that process.

21 Q. Was there additional information related to the  
22 transmission of data from the NIT to the government when it  
23 was executed in this case that's been made available?

24 A. Yes. When the NIT was executed and ran the instructions  
25 that it was authorized to run on Mr. Matish's computer, it

—D. Alfin - Direct—

1 transmitted items of evidence to the government. Those items  
2 are what is listed in the attachments to the NIT search  
3 warrant, and that data stream was collected and preserved in  
4 its entirety. It can be reviewed. I have reviewed it  
5 myself. I have confirmed that the information in that data  
6 stream matches exactly what has been turned over to defense.  
7 It matches exactly what the FBI was authorized to collect.

8 Importantly, it can be reviewed. It can be used in  
9 conjunction with the source code that we've turned over to  
10 verify that what the NIT generates is the same as what the  
11 FBI has collected and turned over.

12 Q. And that was something that you provided this morning and  
13 are aware has been turned over to defense counsel?

14 A. Correct, it was provided on a disk today.

15 THE COURT: When?

16 THE WITNESS: Just before the hearing, Your Honor.

17 THE COURT: What hearing?

18 THE WITNESS: This hearing, Your Honor.

19 THE COURT: I thought you had already done that.  
20 You just did it today?

21 THE WITNESS: We turned over the source code for the  
22 NIT previously, Your Honor. What we turned over today is the  
23 copy of the network data that went from Mr. Matish's computer  
24 to the government. It reflects the same information --

25 THE COURT: In response to the NIT?

—D. Alfin - Direct—

1 THE WITNESS: Yes, Your Honor.

2 THE COURT: All right.

3 BY MS. GRATTON:

4 Q. And you've testified that computers have been made  
5 available. Are you familiar with any reports generated based  
6 on the analysis of those computers at various times in this  
7 investigation?

8 A. Yes, I read reports from a preview of Mr. Matish's  
9 computer. That preview confirmed that the computer on which  
10 the NIT was executed is, in fact, Mr. Matish's computer. The  
11 information in that report matches what the FBI collected, it  
12 matches what the FBI turned over, and it matches what defense  
13 is able to duplicate with the discovery that they've been  
14 provided.

15 Q. And when was that preview conducted?

16 A. That preview, I was informed, was conducted pursuant to  
17 the search warrant that was executed at Mr. Matish's  
18 residence.

19 Q. And of the information that you described, can you  
20 briefly explain for the Court how it could be used to  
21 determine the full extent of what information was seized  
22 through the operation of the NIT?

23 A. The NIT source code that was turned over can be executed  
24 by defense. They can see exactly what information it  
25 collects, what it generates, and they can compare that to

—D. Alfin - Direct—

1 what has been turned over to the government. If they were to  
2 execute it on Mr. Matish's computer, they would observe that  
3 the information that is collected is, in fact, what the FBI  
4 collected pursuant to the NIT search warrant.

5 Q. Would that process also reveal whether any additional  
6 information, such as images or other content, were  
7 transmitted as part of the NIT?

8 A. It would. If you were to execute the NIT, compile the  
9 source code, and run it on the computer, you would be able to  
10 observe if any images or other files were being pulled from  
11 somewhere else on the Internet. That is not a function of  
12 the NIT, but the discovery that we provided can confirm that.

13 Additionally, because we provided the full and not  
14 redacted data stream as a result of the execution of the NIT,  
15 that data stream can be reviewed, and it can confirm that  
16 there were no images transmitted, or videos, or any other  
17 files as a result of the NIT.

18 I have reviewed the data stream myself and confirmed  
19 that no files of any sort were transferred to Mr. Matish's  
20 computer as a result of the NIT.

21 Q. How could the information provided or made available to  
22 the defendant be used to determine whether the NIT interfered  
23 with or compromised any data or computer functions?

24 A. In declarations that have been submitted on behalf of  
25 Mr. Matish there are allegations that the NIT could have

D. Alfin - Direct

1       installed software or could have made changes to the  
2       computer. The NIT did not install software, it did not make  
3       changes to the computer; however, defense has everything that  
4       they need to verify these claims. They have the NIT itself  
5       that they can review to confirm that it does not make changes  
6       to the computer. They also have access to Mr. Matish's  
7       computer. They can review it, they can analyze it, and they  
8       can see if there's anything on the computer, any settings  
9       that were changed or anything else as a result of the NIT.

10           Again, the NIT did not do anything outside of the  
11       scope of what the NIT warrant authorized; however, Mr. Matish  
12       has all the information that he needs available to him to  
13       confirm or dispute those claims.

14       Q. And what about determining the accuracy of the  
15       information that the NIT generated?

16       A. In one of the declarations that was submitted on behalf  
17       of Mr. Matish by Dr. Soghoian, it is alleged that because the  
18       NIT sent data over the regular Internet and not encrypted  
19       that the authenticity of the data could not be verified.  
20       This is incorrect.

21           It also fails to acknowledge that the NIT was, in  
22       fact, sent to Mr. Matish's computer over the Tor network,  
23       which is encrypted.

24           It also included with it a unique identifier. And,  
25       so, because that unique identifier was sent to Mr. Matish's

D. Alfin - Direct

1 computer over an encrypted connection, we know that it was  
2 not tampered with at that point in time. Additionally, the  
3 transmission that was received from the government contained  
4 that same unique identifier, so the government was able to  
5 confirm when it received the information generated by the NIT  
6 that it had not been tampered with.

7 Additionally, in order for an individual to have  
8 successfully tampered with the NIT data stream, that  
9 individual would have had to have known about the FBI's  
10 operation, known the IP address that the FBI was utilizing.  
11 They also would have had to have physical access or some  
12 other kind of access to Mr. Matish's computer to learn the  
13 MAC address and other information from his computer. They  
14 would have had to have known that Mr. Matish was a member of  
15 the Playpen Web site, they would have had to have known when  
16 Mr. Matish was going to access the Playpen Web site, and they  
17 would have had to have a capability to intercept the FBI data  
18 stream and alter it in the course of about a second, because  
19 that's how long the NIT data stream took to transfer.

20 No such individual or organization exists who could  
21 have known those things and would have had the capability to  
22 alter the data in that manner.

23 Q. On that point, for example, when did the FBI's operation  
24 become public?

25 A. FBI's operation was conducted approximately between

—D. Alfin - Direct—

1 February 20, 2015, and March 4, 2015. The first public  
2 reporting on the operation, I believe, was approximately June  
3 of that year, several months after the FBI's operation had  
4 concluded, and there is no information or evidence to suggest  
5 that anyone knew about the FBI's operation while it was  
6 ongoing.

7 THE COURT: Did you say from February 20th to  
8 March 4th?

9 THE WITNESS: Yes, Your Honor.

10 THE COURT: Of '15?

11 THE WITNESS: Yes, Your Honor.

12 BY MS. GRATTON:

13 Q. Would encryption of the data as it was transmitted from  
14 the computer to the government -- what effect, if any, would  
15 that have had on the utility of the data going forward?

16 A. It would have not completely made the network data  
17 useless, but it would have hurt it from an evidentiary  
18 standpoint.

19 Because the FBI collected the data in a clear text,  
20 unencrypted format, it shows the communication directly from  
21 Mr. Matish's computer to the government. It can be read; it  
22 can be analyzed. It was collected and provided to defense  
23 today, and they can review exactly what the FBI collected.

24 Had it been encrypted, it would not have been of the  
25 same value, because the encrypted data stream itself could

—D. Alfin - Direct—

1 not be read. In order to read that encrypted data stream, it  
2 would have to first be decrypted by the government, which  
3 would fundamentally alter the data. It would still be valid,  
4 it still would have been accurate data; however, it would not  
5 have been as forensically sound as being able to turn over  
6 exactly what the government collected.

7 Q. And on the question of chain of custody, that data stream  
8 includes the unique identifier?

9 A. Correct. The chain of custody of the evidence is valid,  
10 the digital chain of custody, as it's referred to. Because  
11 the data stream included a unique identifier, that unique  
12 identifier was sent to Mr. Matish's computer over the  
13 encrypted Tor network. It came back with the NIT results.  
14 It was not changed in transit, and it did, in fact, report  
15 accurate data from Mr. Matish's computer.

16 And more important is the fact that the defense does  
17 not have to take the government's word for it. They have all  
18 the tools that they need to recreate exactly what the  
19 government used by using the NIT source code, comparing it to  
20 the network packet capture, and comparing it to the data that  
21 was provided in discovery. The defense has everything they  
22 need to recreate every step of this process to validate the  
23 data that we have provided.

24 Q. And when you say that the data was accurate, have you  
25 reviewed information from the computer seized in this case

—D. Alfin - Direct—

1 and compared it to the NIT results?

2 A. I have. I have reviewed that data and confirmed that the  
3 information that the NIT collected does in fact match  
4 information from Mr. Matish's computer.

5 THE COURT: How much longer do you expect your brief  
6 evidence to take?

7 MS. GRATTON: If I may just have five more minutes,  
8 Your Honor.

9 THE COURT: All right.

10 BY MS. GRATTON:

11 Q. Have you reviewed the unique identifiers generated  
12 through the operation of the NIT in all cases such as this?

13 A. Yes, I've confirmed that every unique identifier that was  
14 generated in this investigation was, in fact, unique. There  
15 were no duplicate identifiers generated.

16 Q. Would a disclosure of -- well, have you reviewed the  
17 charges pending in the superseding indictment in this case?

18 A. I have.

19 Q. Are any of them tied to child pornography found on  
20 Mr. Matish's computer?

21 A. No. The charges in the matter at hand stem from the  
22 activity of the Broden user account on the Playpen Web site,  
23 which is corroborated by statements made by the defendant.

24 Q. Are you aware of whether child pornography was, in fact,  
25 found on any of these devices?

—D. Alfin - Direct—

1 A. I have been informed that child pornography was found on  
2 devices belonging to Mr. Matish.

3 Q. Where?

4 A. It was found in unallocated space on his computer, and  
5 what that means is the images of child pornography were  
6 placed on his computer at some point in time and then  
7 deleted. The FBI was able to recover them using forensic  
8 software.

9 Q. Would there be any information in files found in that  
10 location regarding their source or when they were placed on  
11 the computer?

12 A. No.

13 Q. Would any further disclosure of information related to  
14 how the NIT was executed reveal where that information came  
15 from?

16 A. There is nothing else in the government's possession that  
17 could shed light on where the images of child pornography on  
18 Mr. Matish's computer came from.

19 Q. Did the NIT have any other functionality beyond that  
20 described in the warrant, such as turning on webcams?

21 A. No. The functionality of the NIT was described very  
22 specifically in the NIT warrant. It did not have any  
23 functions outside of what was described in the NIT warrant.  
24 It did not install any software, it could not remotely take  
25 control of the computer, there was nothing left behind. No

—D. Alfin - Direct—

1 settings on the computer were altered.

2 Q. And could that be verified through a review of the NIT  
3 code and the computer as you've testified and as described in  
4 the declaration?

5 A. Yes.

6 Q. Have you performed such reviews in the past in other  
7 cases?

8 A. I have in other cases conducted analyses of computers  
9 that were thought to be infected with either malware or  
10 viruses or other software. I have conducted that review on  
11 my own. I have been successful in finding such malware and  
12 analyzing it.

13 Mr. Matish has everything available to him to  
14 conduct such an analysis, should he decide to do so.

15 Q. And the process for that is described in the declaration  
16 you submitted to the Court?

17 A. That's correct.

18 Q. And, finally, would you describe the NIT as malware?

19 A. No. The declaration of Dr. Soghoian disputes my point  
20 from my declaration that I do not believe the NIT should be  
21 considered malware, but he fails to address the important  
22 word that makes up malware, which is "malicious."

23 "Malicious" in criminal proceedings and in the legal  
24 world has very direct implications, and a reasonable person  
25 or society would not interpret the actions taken by a law

\_\_\_\_\_  
D. Alfin - Cross

1 enforcement officer pursuant to a court order to be  
2 malicious. And for that reason I do not believe that the NIT  
3 utilized in this case pursuant to a court order should be  
4 considered to be malware.

5 Q. Would it have fundamentally altered the defendant's  
6 computer?

7 A. No, and the defendant has everything he needs available  
8 to him to dispute that claim. There's nothing to dispute,  
9 but he can try to if he wants to. He has his computer  
10 available to him. He also has the NIT available to him to  
11 review.

12 Q. Thank you.

13 MS. GRATTON: Would you please answer any questions  
14 that the defense or the Court may have.

15 MR. GRINDROD: May I inquire, Your Honor?

16 THE COURT: You may.

17 CROSS-EXAMINATION

18 BY MR. GRINDROD:

19 Q. Agent Alfin, I'm going to jump around a little bit. I'll  
20 try to let you know where I'm going.

21 So you started off talking about various items of  
22 evidence that have been made available to the defense.

23 A. Yes.

24 Q. Now, you're aware that the defense requested all this  
25 information about the NIT and the code and the computer

-----D. Alfin - Cross-----

1 programming back in March, right?

2 A. I don't know the exact date, but I'm aware that these  
3 requests have been made.

4 Q. Okay. And you talked about the fact that the government  
5 made available the source code for the NIT, which has been  
6 referred to also -- we refer to it as the payload.

7 Do you know what I'm talking about?

8 A. The defense has. You have referred to it in different  
9 terms. We have turned over what the government has defined  
10 as the NIT in its entirety.

11 Q. Okay. And you're aware that the first time that the  
12 government agreed to produce that particular data was in its  
13 response to this motion to compel?

14 A. I assume that's the case. I don't know exactly what date  
15 it was provided on, but I know it was turned over.

16 Q. And then you talked about a data stream being made  
17 available, right?

18 A. Yes.

19 Q. And you're aware that the first time that the government  
20 agreed to produce that data was in its surreply to the motion  
21 to compel.

22 A. I don't recall the first time that that data was made  
23 available, but I know it has been made available and has been  
24 turned over.

25 Q. As of --

-----D. Alfin - Cross-----

1 A. As of today.

2 Q. -- 20 minutes ago, correct?

3 A. Yes. To the best of my knowledge, it was not turned over  
4 prior to that.

5 Q. And you talked about access to Mr. Matish's computer  
6 itself being, perhaps, a substitute for some of the other  
7 data that the defense is requesting, right?

8 A. Everything that the defense has requested can be verified  
9 with the discovery that is available.

10 Q. Now, the problem with that, right, is that a computer is  
11 a malleable object, right, from a data perspective, right?

12 A. Data on a computer can change.

13 Q. And, so, there are a number of sophisticated forensic  
14 techniques for recovering data from computers, right?

15 A. There are.

16 Q. But, at bottom, once a particular bit, once a particular  
17 data point is written over, it's gone forever, right?

18 A. After data has been overwritten it can be very difficult  
19 or impossible to recover, yes.

20 Q. Okay. And so the NIT in this case, the exploit, was  
21 deployed in February, right?

22 A. I believe it was in February, yes.

23 Q. And law enforcement did not actually go and seize  
24 Mr. Matish's computer until much later that summer, and I  
25 believe it was July, right?

D. Alfin - Cross

1 A. I don't remember the exact date, but, that's correct, I  
2 believe it was several months later.

3 Q. So there's a significant time gap between when the  
4 government ran its exploit, right, broke into Mr. Matish's  
5 computer, and when it actually physically went and seized the  
6 computer, right?

7 A. There was a period of several months in between the NIT  
8 identifying Mr. Matish and the search warrant that was  
9 executed at his residence, yes.

10 Q. Okay. So if the government's use of the exploit made  
11 Mr. Matish's computer vulnerable to some sort of other  
12 malware attack -- right? -- then that evidence may have  
13 existed on the computer at some point during that months-long  
14 period but may not exist now, based on the computer as  
15 recovered in July, right?

16 A. The defense has said in its declaration that the NIT may  
17 have made fundamental changes to Mr. Matish's computer;  
18 however, the preview reports that I have read that are also  
19 available to defense review show that the important  
20 information on the computer remained the same between the  
21 time that the NIT identified his computer and the time that  
22 the search warrant was executed.

23 Additionally, it's my understanding the defense has  
24 made no effort to actually analyze his computer to search for  
25 any fundamental changes or any other alterations to the

-----D. Alfin - Cross-----

1 computer that are alleged.

2 Q. Okay. So my question was if there was some malware or  
3 someone exploited the vulnerability created by the FBI in  
4 February --

5 A. The FBI did not create any vulnerability.

6 Q. I want you to assume that they did for purposes of my  
7 question, okay?

8 A. They didn't. I can't answer your question like that.

9 Q. Well, you're testifying as an expert in this case,  
10 correct?

11 A. I don't believe I was qualified as an expert.

12 Q. So none --

13 A. I can --

14 Q. None of the opinions, none of the testimony you're  
15 offering in this case, is based on any sort of expertise?

16 A. No, it certainly is. I'm just -- for the record, I don't  
17 believe I was officially qualified as an expert. I know  
18 different districts handle that differently. I just want to  
19 make sure I'm not misrepresenting my position.

20 THE COURT: Well, I think when you file a  
21 declaration in response to another person's expert  
22 declaration that you're acting as an expert.

23 THE WITNESS: Understood. Different districts --

24 THE COURT: So I think that Counsel can ask you a  
25 hypothetical question which, if you are able to answer, you

-----D. Alfin - Cross-----

1 should answer.

2 THE WITNESS: Understood, Your Honor.

3 THE COURT: So go ahead with your question.

4 MR. GRINDROD: Thank you, Your Honor.

5 BY MR. GRINDROD:

6 Q. So I'm asking you for purposes of this question to assume  
7 that the FBI did create some sort of vulnerability when it  
8 deployed the exploit in this case on Mr. Matish's computer.

9 A. Okay.

10 Q. That would have taken place back in February, correct?

11 A. Correct.

12 Q. And if that vulnerability led to some other malware or  
13 some other security breach in Mr. Matish's computer, the  
14 evidence of that breach or of that other malware may have  
15 existed on Mr. Matish's computer at some time between  
16 February and July but may have disappeared by the time the  
17 government seized that computer in July, right?

18 A. In this theoretical situation that describes the events,  
19 that did not happen. Data could be deleted. It's certainly  
20 possible.

21 Q. So the answer to my question is "yes," correct?

22 A. The answer to your question is that data can be deleted.

23 Q. And you would agree with me that when hackers or other  
24 people use malware or try to surreptitiously get onto  
25 someone's computer those programs are often designed in a way

-----D. Alfin - Cross-----

1 to try to actively cover up tracks, right? They try not to  
2 leave evidence behind of the fact that they were there,  
3 right?

4 A. Some malware is designed with those features, yes.

5 Q. So...

6 MR. GRINDROD: The Court's indulgence, Your Honor.

7 (There was a pause in the proceedings.)

8 BY MR. GRINDROD:

9 Q. So let's talk about -- at various points in your direct  
10 testimony you said that if you were the defense expert you  
11 would do X, Y, or Z. Do you remember those statements?

12 A. Yes, I remember them.

13 Q. And you also testified that in your capacity as, I guess,  
14 a government expert in this case you have gone and looked at  
15 the data, the evidence itself, and analyzed it and then made  
16 some sort of conclusion or statement in your declarations or  
17 in your testimony today, right?

18 A. Yes, that's true.

19 Q. And you mentioned at various times that if you were the  
20 defense expert you would confirm that you would use the data  
21 provided to confirm that the data did what the FBI says it  
22 did, right?

23 A. I said that I would use the evidence that the government  
24 has provided in discovery to confirm that the evidence that  
25 we collected and made available is an accurate representation

D. Alfin - Cross

1 of what the NIT actually sent from Mr. Matish's computer.

2 Q. You testified on direct that the use of -- that the  
3 analysis of the NIT would allow a defense expert to confirm  
4 that it does exactly what the FBI says it does.

5 Do you remember that testimony?

6 A. Yes. That, combined with the other evidence available,  
7 but, yes, I said that.

8 Q. And what you're saying, right, is based on the data you  
9 have provided, some data, that a defense expert,  
10 technological expert, could look at the data to determine  
11 whether, in fact, what the FBI says they did actually is what  
12 they did, right?

13 A. Yes, that's correct.

14 Q. Okay. And you would agree with me that that is a proper  
15 role for a forensic expert.

16 A. Yes.

17 Q. Okay. You would also agree with me that the government  
18 has not produced some of the data, including the exploit, in  
19 this case, correct?

20 A. There was an exploit used in this case that has not been  
21 turned over because it is immaterial.

22 Q. And you agree that it is possible for an exploit to make  
23 fundamental alterations to a computer system.

24 A. Yes. In my declaration I stated that an exploit -- not  
25 the one used by the government -- could make alterations to a

—D. Alfin - Cross—

1 computer system; however, the one the government used did  
2 not.

3 Q. Okay. So that part of your statement, the "however" --  
4 right? You say, "however." An exploit can do this; however  
5 yours didn't, right?

6 A. Correct, and that can be confirmed by analyzing  
7 Mr. Matish's computer, which is available to your defense to  
8 review.

9 Q. Well, except that my client's computer may not contain  
10 that data. You just testified it may have been overwritten,  
11 right?

12 A. It contains the same data that the NIT collected back in  
13 February. We've reviewed that report.

14 Q. So you would agree with me that with respect to some of  
15 the data you've agreed to produce you say a defense expert  
16 should look at the data and, based on looking at the data,  
17 they can confirm whether or not the technology actually did  
18 what the FBI says it did, right?

19 A. Yes, they should look at what we provided to confirm that  
20 what we've provided does what we say it does.

21 Q. And you would agree with me that the government, having  
22 not produced the exploit -- the defense experts cannot look  
23 at the exploit to see if the exploit did what you say it did,  
24 right?

25 A. The exploit, again, would shed no light on what the

-----D. Alfin - Cross-----

1 government did. It would not --

2 Q. Let me stop you there and ask a follow-up, if I can.

3 A. Okay.

4 Q. You say the exploit would shed no light on what the  
5 government did. The government deployed this exploit,  
6 correct?

7 A. The government used the exploit to deploy the NIT.

8 Q. And I believe you used the analogy that this exploit is  
9 like a way of picking a lock, right?

10 A. Yes. A more accurate analogy may be going in through an  
11 open window. As I've stated in my declaration, there was a  
12 vulnerability on Mr. Matish's computer. The FBI did not  
13 create that vulnerability. That vulnerability can be thought  
14 of as an open window. So we went in through that open  
15 window, the NIT collected evidence, and then left. We made  
16 no change to the window.

17 Looking at that window, telling you what window it  
18 was, you can look at the window all day long. It gives you  
19 no insight into what the FBI did or what evidence was seized.  
20 In order to know that you have to analyze the NIT, which was  
21 turned over in its entirety.

22 Q. So let's not confuse analogies. Let's go back to the one  
23 you used in your declaration about picking the lock.

24 A. Okay.

25 Q. So you're telling us that you know exactly how the

\_\_\_\_\_  
D. Alfin - Cross

1 government picked the lock on the front door to Mr. Matish's  
2 computer, right?

3 A. I know information about how the FBI deployed the NIT.

4 Q. And that's because you've seen the data that makes up the  
5 exploit, right?

6 A. No, I have not.

7 Q. So you're offering sworn statements about what the  
8 exploit did or didn't do. What is the basis for your  
9 testimony?

10 A. I have executed the NIT, which included utilizing the  
11 exploit on a computer under my control. I confirmed that it  
12 collected the information that it was authorized to collect,  
13 and I confirmed that it did not make any fundamental changes  
14 to my computer.

15 Q. So you didn't even look at the actual code, at the actual  
16 data, you just tried to observe the effects of executing the  
17 code?

18 A. I have not viewed the exploit myself, nor have I ever  
19 claimed to or made any implication that I have.

20 Q. Well, you make a number of explanations about what the  
21 exploit is and what it does and doesn't do.

22 A. Yes.

23 Q. But it's your testimony today that you've never even  
24 looked at this data that the defense is requesting.

25 A. You can use a computer without knowing how to build a

—D. Alfin - Redirect—

1 computer and see what the computer does.

2 I never claimed to have looked at the exploit, nor  
3 would there be any need to, because, again, as stated  
4 previously, it is immaterial.

5 MR. GRINDROD: No further questions, Your Honor.

6 MS. GRATTON: If I may just briefly address a couple  
7 of points, Your Honor, very briefly.

8 REDIRECT EXAMINATION

9 BY MS. GRATTON:

10 Q. The defense asked you about a hypothetical in which the  
11 FBI created a vulnerability. Is there a way to test whether  
12 any such vulnerability was created?

13 A. Yes. If they want to see if there were any fundamental  
14 changes or vulnerabilities on Mr. Matish's computer, they can  
15 review Mr. Matish's computer, which they have declined to do  
16 thus far.

17 Additionally, they can look at the NIT source code,  
18 which we have provided in its entirety, and confirm that it  
19 does not make any changes to the computer or open up  
20 vulnerabilities.

21 Q. And the information gathered by the NIT, to briefly  
22 summarize, was the operating system, the host name, the user  
23 name, the MAC address, the unique identifier, whether the NIT  
24 had been deployed to it before, and then also the IP address  
25 disclosed in the transmission of that information back to the

D. Alfin - Redirect

1       FBI?

2       A. Whether or not the NIT had been deployed to the computer  
3       previously was information tracked by the government.  
4       Mr. Matish's computer would have no way of knowing that  
5       itself, but, yes, those are the items listed from the warrant  
6       attachment.

7       Q. Are any of those items -- I believe you testified to the  
8       MAC address. Can that be changed?

9       A. It can be --

10            MR. GRINDROD: Objection, Your Honor. This is all  
11       outside the scope and asked and answered.

12            MS. GRATTON: Your Honor, the defense is arguing  
13       that some hypothetical attack on Mr. Matish's computer  
14       through a hypothetical vulnerability resulted in significant  
15       changes to his computer that may no longer exist, and, so,  
16       I'm trying to determine whether the information at issue,  
17       which are the items collected by the NIT, could have been  
18       changed.

19            There's been testimony that they did not change, but  
20       whether a MAC address or an operating system is subject to  
21       complete hack and overwritten, that may have vanished in the  
22       months between the execution of the NIT and the seizure of  
23       the defendant's computer, as Counsel suggested on cross.

24            THE COURT: Well, I think he's already answered that  
25       question.

1 MS. GRATTON: Very well.

2 BY MS. GRATTON:

3 Q. And although you've not reviewed the exploit source code,  
4 are you familiar with the operation of the NIT in this case?

5 A. I am.

6 Q. And you --

7 MS. GRATTON: No further questions.

8 THE COURT: All right. You may step down.

9 THE WITNESS: Thank you, Your Honor.

10 THE COURT: All right, Mr. Grindrod. It's your  
11 motion, so I'll hear first from you.

12 MR. GRINDROD: Your Honor, I would first direct the  
13 Court's attention to the decision in *Michaud*, which since the  
14 last time we were here I've supplemented the record with the  
15 order from that case that addressed the discoverability of  
16 this same information and the transcript regarding the  
17 same --

18 THE COURT: You did, but it didn't really give any  
19 reason for the opinion.

20 MR. GRINDROD: Well, Your Honor --

21 THE COURT: It just said he had studied it before  
22 and mentioned a series of amendments and said, that's it.

23 MR. GRINDROD: Well, Your Honor, I would just  
24 note --

25 THE COURT: So the decision is helpful, but the

1 rationale is absent.

2 MR. GRINDROD: I understand the Court's position.

3 The Court in that case did rely on expert  
4 declarations that were very similar to and in some cases  
5 drafted by the same experts in this case, which I do think is  
6 probative, but I understand the Court's position on that.

7 I would also note the government raises in its  
8 surreply that there is some meaningful difference in the  
9 circuit standard. I think that's a bit of a red herring,  
10 Your Honor. Under either the Ninth Circuit standard or the  
11 Fourth Circuit standard, which we agree is set out in *Caro*,  
12 there is a strong indication that this evidence will play a  
13 role in uncovering admissible evidence, aiding in witness  
14 testimony, and corroboration and/or impeachment.

15 Your Honor, I'm going to use a couple of analogies,  
16 because I think it's important not to get too lost in the  
17 weeds of the technology here. But I think it's appropriate  
18 to view this code as analogous in some ways to a confidential  
19 informant or the underlying DNA analysis that we see in maybe  
20 a more common case. And the fundamental disagreement between  
21 the government and the defense in this case is whether the  
22 defense is entitled to the evidence or, alternatively,  
23 whether the defense is entitled to the government's  
24 description of or assurances about what the evidence will  
25 show.

1           It's our position, Your Honor, that the government  
2 cannot simply say, we've reviewed the evidence, or, in the  
3 case of Agent Alfin, I haven't actually looked at the code  
4 that you want, but I can still tell you you don't need it.

5           We've set out through our expert declarations  
6 exactly why this information is critical, and the government  
7 is saying, no, we've looked at it, we've analyzed it; our  
8 experts say you wouldn't be able to make a meaningful trial  
9 defense based on this information. But in some ways, Your  
10 Honor, that's the same as saying, we're not telling you who  
11 our confidential informant is. You don't need to talk to  
12 him, because we're telling you he's believable and everything  
13 he's saying is true. You don't need to look at the DNA tests  
14 from the lab, because we're telling you it's a match, and  
15 we're telling you the tests were fine.

16           The government has the evidence --

17           THE COURT: Well, now, among the things that were in  
18 your expert declaration was that you could tell -- or you  
19 wanted to examine the exploit to determine if the information  
20 sent back from the defendant's computer to the government's  
21 computer was compromised.

22           MR. GRINDROD: That's one reason we need the  
23 exploit. That's one reason we need that.

24           THE COURT: Now, what information do you have that  
25 that information was compromised in transit?

1                   MR. GRINDROD: Well, we know, Your Honor, that it  
2 was susceptible to being tampered with, and --

3                   THE COURT: Why? How do you know that?

4                   MR. GRINDROD: Well, that's based on Agent Alfin's  
5 testimony at the suppression hearing. We know that this  
6 information was not sent in encrypted form, and Dr. Soghoian  
7 sets out in his declaration that that's very important,  
8 because when information is sent through unencrypted channels  
9 it's particularly susceptible to being tampered with. So  
10 that's one reason, Your Honor.

11                  But the other reason, Your Honor --

12                  THE COURT: Well, they also said that the best  
13 practices required that it be encrypted.

14                  MR. GRINDROD: That's what our expert would say,  
15 Your Honor, yes -- or has said.

16                  THE COURT: Why would that be the case?

17                  MR. GRINDROD: To prevent tampering with the  
18 evidence. I mean, this is analogous to -- I mean, there's a  
19 crime scene. Certain evidence is collected, and rather than  
20 bagging and labeling it and following established techniques  
21 for how evidence is to be collected and transferred back to,  
22 you know, the server, which is like an evidence locker, they  
23 just threw everything in the back seat of the cruiser and  
24 drove back. Oh, and, by the way, they won't tell us whether  
25 on the way back they also picked up someone else who rode in

1 the back of the cruiser.

2 I mean, in some ways the government is right that by  
3 maintaining a monopoly on the evidence, by keeping the  
4 evidence secret from the defense, we can't, with absolute  
5 certainty, say that the evidence was tampered with. We can  
6 just say that we know, based on Agent Alfin's declaration,  
7 that it was susceptible to being tampered with and that the  
8 evidence of the government --

9 THE COURT: Well, your experts seemed to indicate  
10 that they thought it could be tampered with as well.

11 MR. GRINDROD: That's correct, Your Honor.

12 THE COURT: And, therefore, it should have been  
13 encrypted.

14 MR. GRINDROD: That's correct, Your Honor.

15 THE COURT: Because if you don't encrypt it, anybody  
16 can tamper with it.

17 MR. GRINDROD: I think that's correct, Your Honor.

18 And, also, I think the exploit is particularly  
19 important here, Your Honor. And the government concedes that  
20 an exploit -- although, they don't say theirs did this --  
21 that an exploit can create critical vulnerabilities, make  
22 fundamental changes to a computer system. And Agent Alfin  
23 somehow, without having actually looked at the code, is able  
24 to offer under-oath statements that their exploit did not do  
25 those things. But, again, this notion of unlocking --

1                   THE COURT: Your experts have not examined the  
2 defendant's computer.

3                   MR. GRINDROD: That's correct, Your Honor.

4                   THE COURT: But the government has offered them the  
5 opportunity to do that.

6                   MR. GRINDROD: That's correct, Your Honor, and we've  
7 actually very recently had some conversations about getting a  
8 forensic copy of the computer to better analyze the parts of  
9 the code that the government has produced. But we don't  
10 agree that that's a substitute, I mean, for the very reasons  
11 that Agent Alfin said on the stand; that there was --

12                  THE COURT: Well, if you examined the defendant's  
13 computer and hypothesized there had been some malware  
14 inserted on the computer in this gap period you're talking  
15 about, maybe it would still be on there, and maybe your  
16 experts could find it.

17                  MR. GRINDROD: That's true, maybe, but --

18                  THE COURT: Oh, well, "maybe's" are what we're  
19 talking about here, because maybe there's malware on it, and  
20 maybe they could have found it, if there was. So it would  
21 seem --

22                  MR. GRINDROD: But what's critical -- sorry, Your  
23 Honor.

24                  THE COURT: Don't talk over me.

25                  MR. GRINDROD: Yes, Your Honor.

1                   THE COURT: It seems to me that by examining the  
2 computer they would have had everything to gain and nothing  
3 to lose. They might have found something that would give  
4 them a factual basis for saying that they need the source  
5 code. Maybe they would; maybe they wouldn't. But if they  
6 did, it would certainly strengthen their position in asking  
7 for the code, wouldn't it?

8                   MR. GRINDROD: I think that's probably right, Your  
9 Honor.

10                  THE COURT: All right. Well, I don't understand why  
11 they wouldn't have taken advantage of that opportunity before  
12 today's hearing.

13                  MR. GRINDROD: Well, Your Honor, it's unlikely  
14 that -- I mean, Agent Alfin touched on this, but, I mean, the  
15 malware that would have taken advantage of the vulnerability  
16 that may have been created by the government is, in all  
17 likelihood, designed not to be found, and, so, the fact  
18 that --

19                  THE COURT: I think what I'm saying is they had  
20 everything to gain by examining the computer and nothing to  
21 lose. What could they have lost by examining it?

22                  MR. GRINDROD: Well, a lot of money. But, I mean,  
23 Your Honor, the fact of the matter is that --

24                  THE COURT: Well, you haven't asked for any money to  
25 cover their cost of examining the computer, have you?

1                   MR. GRINDROD: No, Your Honor, but if the government  
2 wants to pay for our expert to conduct a full forensic  
3 analysis and then, if and when they don't find anything,  
4 they'll agree to produce the exploit, then we would agree to  
5 that process. I mean, the fact that --

6                   THE COURT: Well, I don't understand why they  
7 wouldn't do that, because they've got everything to gain and  
8 nothing to lose by examining his computer. I mean, they  
9 might find -- they said, well, maybe there was another source  
10 for the pornography other than directly from Playpen.

11                  Well, if they examined the computer maybe they would  
12 find some evidence that there was some other source. Maybe  
13 they would; maybe they wouldn't. But, again, isn't it worth  
14 a try?

15                  MR. GRINDROD: Well, perhaps it is, Your Honor. I  
16 would say that --

17                  THE COURT: And shouldn't they try before they come  
18 here and ask for the source code?

19                  MR. GRINDROD: No, Your Honor, and let me explain.

20                  THE COURT: Why not?

21                  MR. GRINDROD: Well, because --

22                  THE COURT: Because then there might be some basis  
23 in fact for them to believe that they might find something.

24                  MR. GRINDROD: Well, there is a basis in fact to  
25 believe that --

1                   THE COURT: No, I think at this point it's very  
2 speculative.

3                   MR. GRINDROD: Well, if our experts analyzed the  
4 computer and they found nothing, then the exact points that  
5 they've made today are exactly the same.

6                   If they have the exploit, that also could help them  
7 look for --

8                   THE COURT: Well, I mean, if they examined it and  
9 there was no evidence of anything on there in the way of  
10 malware and there was no evidence that there was any breach  
11 or change to the security apparatus on the computer, it would  
12 weaken their case in asking for the source code, wouldn't it?

13                  MR. GRINDROD: No, Your Honor.

14                  THE COURT: It wouldn't?

15                  MR. GRINDROD: And that's the point I'm trying to  
16 make.

17                  So the absence of finding malware on the computer  
18 itself is the expected outcome, even if there was malware on  
19 the computer, and, so, what we need to do --

20                  THE COURT: Well, it sounds to me like, then, that  
21 they're saying that there's not much probability that there's  
22 anything on there.

23                  MR. GRINDROD: Again, I disagree with that  
24 characterization, Your Honor. I think that what they're  
25 saying is that the --

1                   THE COURT: I think what they're saying is they want  
2 to call it -- they want to call NIT malware.

3                   MR. GRINDROD: I don't think that matters at all,  
4 Your Honor.

5                   THE COURT: Absolutely. I one hundred percent agree  
6 with you. So why are they doing it?

7                   MR. GRINDROD: Well, I think the academics get  
8 excited about it, Your Honor. I think there's still a --

9                   THE COURT: I think the academics don't like what  
10 the NIT does.

11                  MR. GRINDROD: They may or may not, but I think,  
12 from the perspective of this case, whether you call it  
13 malware or not is rhetorical, at best. The fact is --

14                  THE COURT: I agree with you, but if that's the case  
15 why have they spent so much time trying to say it's malware?  
16 Because they try to say it's malware, and it seems like in  
17 saying that they're implying that they don't think the  
18 government should have this capability.

19                  MR. GRINDROD: I think that's a normative question  
20 that the experts in this case don't have to reach. Perhaps  
21 Congress --

22                  THE COURT: Well, they seem to have been trying to  
23 reach it whether they need to or not.

24                  MR. GRINDROD: I agree that there are probably some  
25 definitional points in this case that are, perhaps,

1       technically important, but for the Court's purposes in  
2       deciding this motion I don't think need to be resolved one  
3       way or the other.

4                  For example, whether we call this what the  
5       government is requesting, the full source code or the  
6       payload, or -- I mean, everybody now knows what we're talking  
7       about.

8                  THE COURT: Exactly, and I don't think the labels --  
9       no, I agree with you on that. I think labeling it is an  
10      exercise in uselessness, but it's interesting that they spend  
11      so much time trying to so label it.

12                 MR. GRINDROD: Well, I think, Your Honor, as long  
13      as -- I mean, at some point the definitions are only  
14      important for getting everybody on the same page. And I  
15      think, despite some initial confusion, everybody at least now  
16      has a generalized understanding of what exactly it is the  
17      defense wants, what the government won't produce.

18                 And I would agree with the Court that, for today's  
19      purposes, what we call it is probably less important. But  
20      the evidence is still critically important, and that's what  
21      we're asking for, Your Honor, is that the government -- this  
22      notion of picking the lock to the front door of Mr. Matish's  
23      computer is, I think, one that Agent Alfin put forward and  
24      one that is particularly well-suited to demonstrating why we  
25      need this information.

1                   Agent Alfin suggests, without having looked at the  
2 data, that this particular exploit worked in a way where the  
3 lock was picked but then, after the FBI left the computer,  
4 the door was locked behind it; there was no vulnerability  
5 created. But he agrees, and our experts have set forward a  
6 basis, that without looking at the code there's no way to  
7 know whether the door was locked after the FBI left or  
8 whether it was just left unlocked or that the front door was  
9 open so that anyone passing by could walk right in, and it  
10 was obviously kind of advertising the software vulnerability.

11                  But all of those things are questions that can only  
12 be answered if we have the data, and the government not only  
13 refuses to produce the data but refuses to put on any  
14 evidence by anyone who has actually looked at the data. I  
15 mean, they initiated this prosecution based on this  
16 technology, and now they're playing hide-the-ball. And, Your  
17 Honor, I mean, it goes to the fundamental fairness of the  
18 prosecution. If the government is going to initiate a  
19 technology --

20                  THE COURT: Well, of course, the problem is that the  
21 evidence indicates -- or one of the problems is that the  
22 evidence indicates that the defendant entered the Playpen  
23 site before the NIT was instituted.

24                  MR. GRINDROD: I think that's the government's  
25 position, Your Honor.

1                   THE COURT: Yes, well, that's it, and I think the  
2 defendant admitted that in a written statement which the  
3 Court has ruled is admissible. So what you're trying to do  
4 is say, if we got the source code, we could prove that what  
5 the defendant admitted to is wrong.

6                   MR. GRINDROD: What we're saying, Your Honor, is  
7 that whatever evidence the government may have against our  
8 client, he's entitled to a defense under the Constitution.  
9 And the defense we propose to mount is one that is, in part,  
10 at least, based on a technological defense to the  
11 government's technological evidence. And the only way we're  
12 going to be able to mount that defense is to have an expert  
13 to counter the inevitable government expert who is going to  
14 talk about how reliable this NIT was and how it worked and  
15 how it didn't make any fundamental changes to our client's  
16 computer. You know, how is Mr. Matish supposed to challenge  
17 that evidence or test that evidence? This is the adversarial  
18 system in which --

19                  THE COURT: Step one should have been examining his  
20 computer, as the government points out in its brief.

21                  MR. GRINDROD: Your Honor --

22                  THE COURT: And that's -- and I haven't heard any  
23 reason why they didn't do that. And the witnesses have  
24 elected to testify by declaration so that they couldn't be  
25 cross-examined, which is an interesting way of presenting

1       their evidence, but that's the way you've chosen to present  
2       their evidence. So these questions that the Court has,  
3       they're not here to answer them, so the Court has to draw  
4       inferences from what they've done and what they have failed  
5       to do.

6                    MR. GRINDROD: Well, Your Honor, the experts have  
7       not conducted a forensic analysis of the computer because  
8       they haven't been directed to do so by counsel.

9                    THE COURT: Well, it seems to me that they should  
10      have directed counsel that that's what should have been done.  
11      Counsel is not the expert on the computer. Counsel shouldn't  
12      have directed them to search the computer, they should have  
13      directed counsel that the computer should have been searched.

14                  MR. GRINDROD: And, Your Honor, if that was the  
15      appropriate step, then I believe they would have. And that's  
16      my point, Your Honor. I mean, I get that there's some  
17      rhetorical appeal to this notion of looking at the computer.

18                  THE COURT: Well, they didn't do it.

19                  MR. GRINDROD: Because --

20                  THE COURT: And what they failed to do speaks very  
21      loudly.

22                  MR. GRINDROD: Well, Your Honor, again, I mean, I  
23      think that's only -- that's only -- there's no -- if they  
24      looked at the computer, no matter what they found, the answer  
25      is we still need the exploit.

1                   THE COURT: If they looked at the computer, perhaps  
2 there's evidence there indicating that what they say may have  
3 happened is a bit more likely to have happened, if they  
4 looked at the computer and found something to support their  
5 hypotheses. And I think it's a generous term to describe it  
6 as a hypothesis. It could just as well be described as  
7 speculation.

8                   And they could have -- the evidence is perhaps there  
9 for them to have found some lead on the computer. Experts  
10 can do amazing things with computers. I remember the case  
11 where the man took the computer from his place of employment  
12 and put something on there that was called Erase to erase all  
13 his e-mails. And then he took it to the junkyard and beat it  
14 with a sledgehammer. And then it was recovered, and they got  
15 information off of the computer as to his e-mails.

16                  Experts can get a lot off of computers, and I'm at a  
17 total loss to understand why they didn't instruct you that  
18 that should be done.

19                  MR. GRINDROD: Your Honor, I've raised that point  
20 with Dr. Miller, specifically, and the answer is because it  
21 doesn't move the ball forward. I mean, we can spend a bunch  
22 of money --

23                  THE COURT: Well, I think the answer may be that  
24 Dr. Miller is more interested in getting the code than  
25 getting the information.

1                   MR. GRINDROD: I don't know that there's any basis  
2 for that, Your Honor. I mean, he's subject to a protective  
3 order. It's not like he can publish based on any information  
4 that he gained as a result of this.

5                   THE COURT: I think one of your experts has already  
6 published based on information he gained from this sort of  
7 situation, hasn't he?

8                   MR. GRINDROD: I'm not -- I'm not aware of that,  
9 Your Honor. I know Dr. Soghoian has not reviewed any  
10 information that's subject to the protective order in this  
11 case, so I don't believe he would be --

12                  THE COURT: Well, it's clear -- if nothing else is  
13 clear, it's clear that the experts don't like the fact that  
14 the government has this device at their disposal. That's  
15 absolutely clear.

16                  MR. GRINDROD: But these are accomplished academics,  
17 Your Honor, from --

18                  THE COURT: They're hired experts. And the fact  
19 that you have two of them doesn't add to their credibility,  
20 because, quite frankly, you could probably find any number of  
21 them, if you wanted to, who would say the same thing. It's  
22 like Tweedledum and Tweedledee; oh, yes, I agree with  
23 Dr. So-and-so's analysis. Well, I didn't expect him to say  
24 that he disagreed with it, because if he did I don't think I  
25 would be looking at his declaration.

1                   MR. GRINDROD: The government's only expert in this  
2 case is their case agent, who is running this whole  
3 operation. I mean, this is Agent Alfin's show, with hundreds  
4 of prosecutions across the country. I don't know that his --  
5 I mean, the Court can evaluate the credibility of the various  
6 experts, but the testimony of someone who is the lead case  
7 agent --

8                   THE COURT: I mean, are you saying that an expert  
9 who part of his job is being an expert and is not paid  
10 anything extra is to be criticized for that, as opposed to  
11 somebody who is hired to say something?

12                  MR. GRINDROD: Dr. Soghoian is doing this pro bono,  
13 as he states in his declaration.

14                  THE COURT: Well, I guess Agent Alfin is doing it  
15 pro bono, too, because he gets his regular salary. He's not  
16 getting paid extra for being an expert, is he? You can ask  
17 him that, if he's getting paid extra. I guess your guy who  
18 is doing it pro bono is getting a salary, isn't he?

19                  MR. GRINDROD: Your Honor, I'll leave it to the  
20 Court to decide whether Agent Alfin has a stake in the  
21 outcome or --

22                  THE COURT: Well, let's not -- okay.

23                  MR. GRINDROD: Thank you, Your Honor.

24                  MS. GRATTON: Thank you, Your Honor.

25                  I think, as the Court has pointed out in questioning

1 the facts and whether we're dealing with facts or  
2 speculation, really gets to the heart of the issue here,  
3 which is whether the information sought is material, which is  
4 the standard under Rule 16. You know, if the inquiry is  
5 whether it's material, if it's material, is it subject to  
6 privilege, which the government has asserted, and, if so,  
7 whether there's been a compelling need shown sufficient to  
8 overcome that privilege.

9           But on the question of materiality, the defense has  
10 cited a number of purposes for which he claims he needs the  
11 information, including the full extent of the information  
12 seized by the NIT, whether it interfered or compromised any  
13 computer data functions, whether it was accurately described,  
14 the chain of custody, and then the source of the child  
15 pornography found on his computer.

16           THE COURT: Well, it's his job to challenge  
17 everything, isn't it?

18           MS. GRATTON: Yes, of course. I just -- in looking  
19 at the reasons stated for disclosure of what is, essentially,  
20 how the NIT got to his computer. Because he has the computer  
21 instructions that generated the results. He was provided  
22 today a copy of the data stream that shows exactly how those  
23 results were transmitted back to the government. And, as  
24 Agent Alfin testified, he has, with that information, coupled  
25 with the --

1                   THE COURT: Well, he doesn't want to believe what  
2 they say. Is he entitled to check his credibility by getting  
3 the source code?

4                   MS. GRATTON: I think he first has to make a showing  
5 of materiality, which requires under *Caro* that there must be  
6 some indication that the pretrial disclosure would enable him  
7 to significantly alter the quantum of proof in his favor.  
8 And there has to be a threshold showing of the materiality of  
9 the information there, one based on facts and not  
10 speculation.

11                  As the Court has noted, the defendant has not  
12 examined his computers. He's not pointed to anything in any  
13 of the evidence that's been disclosed or made available  
14 indicating that there's any sort of discrepancy or  
15 irregularity in what the government has done, and --

16                  THE COURT: Does it make any difference that the  
17 defendant said that he was responsible for the Broden posting  
18 on Playpen prior to the NIT being deployed? Does that make  
19 any difference?

20                  MS. GRATTON: The government does believe that it  
21 makes a significant difference, because --

22                  THE COURT: Well, it wouldn't make any difference if  
23 the Court's ruling on this motion impacted the Court's ruling  
24 on the invalidity of the NIT search, to begin with, because  
25 then we wouldn't get to the confession, would we?

1 MS. GRATTON: If the Court were to determine --

2 THE COURT: Does the Court's ruling on this  
3 discovery motion impact the Court's ruling on their first  
4 motion to suppress?

5 MS. GRATTON: Based on the fact that the defendant  
6 has provided only speculation that the NIT did not operate in  
7 the way that the government has said that it did, or that it  
8 gathered or transmitted information beyond what's been  
9 disclosed. All of it, as outlined in the government's  
10 response and surreply, is speculation.

11 There's been a significant amount of evidence on  
12 this issue turned over to the defendant, and yet he doesn't  
13 point to anything in the computer instructions saying that  
14 those instructions would have done something other than  
15 what's been represented, that they would have generated  
16 results other than those disclosed, that they transmitted any  
17 information, such as images or other content.

18 So the government's position is that --

19 THE COURT: Well, the FBI could have just gotten  
20 that second warrant to cover their tracks, couldn't they?  
21 Maybe they got the images through the NIT but they realized  
22 that that went beyond the search warrant, so they went and  
23 got a second search warrant to cover their tracks. They  
24 could have done that, couldn't they?

25 MS. GRATTON: Well, the response is twofold. First,

1 there were no images transferred back to the FBI by --

2 THE COURT: Well, I mean, that's what they say,  
3 right. I mean, does the defendant have to believe that?

4 MS. GRATTON: No. He has the data stream as it was  
5 transmitted from his computer to the FBI. He can look at  
6 that to see if there was anything other than the NIT results  
7 transmitted back to --

8 THE COURT: Well, they're saying that if they had  
9 the source code it may show that they got something else  
10 other than --

11 MS. GRATTON: The source code did not collect or  
12 transmit information. As Agent Alfin testified, it allowed  
13 the FBI to enter an open window.

14 THE COURT: The source code allowed them to enter  
15 the open window, but it didn't play a part in the information  
16 they gathered. That's what they said. How do they test the  
17 accuracy of that information?

18 MS. GRATTON: The computer instructions, if they  
19 recreate those and execute them on the defendant's computer,  
20 will generate the same results. And they can test that. If  
21 they ask to review forensically the computer, they can  
22 analyze it for the presence of any malware. They can execute  
23 a copy of the NIT that's been provided and determine if it  
24 does anything other than it said it would do.

25 If the Court were to order, as the defendant

1 describes, the payloads, any and all payloads, delivered to  
2 the defendant's computer as --

3 THE COURT: Well, the difficulty in using language  
4 like "payloads" is everybody uses a different description,  
5 and it gets confusing to the Court reading all this --

6 MS. GRATTON: If the Court were to order the  
7 government to provide all the source code that gathered or  
8 transmitted information from Mr. Matish's computer to the  
9 government, I could stand here today and tell the Court that  
10 the government has already provided that information. So the  
11 exploit at issue is not -- it didn't collect, it didn't  
12 transmit information.

13 And the question about the child pornography found  
14 on the computer, the FBI did get a second search warrant.  
15 They got a search warrant for the residence that --

16 THE COURT: Well, I know they did, but maybe they  
17 did that just to cover their tracks, huh?

18 MS. GRATTON: The defense can review the data stream  
19 and see. The only -- again, the Court could order us to  
20 disclose the instructions that gathered or transmitted  
21 information and all transmissions from the defendant's  
22 computer, and we have disclosed those. The defense can  
23 review them and, if any such evidence exists, could highlight  
24 that for the Court.

25 With respect to the computer instructions, Counsel

1 has had those for some time. Admittedly, the network stream  
2 was produced this morning. There was -- between the two  
3 hearings counsel for both sides were out and, at the earliest  
4 time possible, discussed the production of the stream, and it  
5 was brought here today in accordance with the agreement that  
6 we reached. But the defense can analyze that and determine  
7 whether any images were sent back, whether the FBI was trying  
8 to cover its tracks by finding the image through a forensic  
9 examination of his computer after the search.

10           But I think the most important point about those  
11 images and one that is, perhaps, not covered as it should  
12 have been in the government's briefing is that, as testified  
13 to here today, they were in unallocated space, they had been  
14 deleted, and none of the charges against the defendant are  
15 based on anything recovered from his computer. The NIT was  
16 used to identify and locate him, as the Court is well  
17 familiar from its consideration of the first and third  
18 motions to suppress.

19           The child pornography on the computer does not serve  
20 as the basis for any charge, and the defense can look at the  
21 information that was collected through the NIT at various  
22 points, they can see the computer instructions, they can see  
23 the network stream of the results and the results as  
24 maintained and turned over by the government in a copy of the  
25 user report and see that all of that is the same. And not

1 only is that the same, but later reviews of the defendant's  
2 computer identified the same information. The preview done  
3 at the time of the search shows the same operating system,  
4 the same information, as does the later forensic report, to a  
5 certain extent. And the defense itself can go and review the  
6 information, and if it's the same at every point there's no  
7 reason to think that it was changed.

8                 And, as Agent Alfin testified, the transition from  
9 Mr. Matish's computer to the government included a unique  
10 identifier that the FBI verified had not been changed. And  
11 he also testified about all of the things that would have to  
12 occur for any kind of tampering with that transmission to  
13 have taken place, including an extensive amount of knowledge  
14 that would have had to have been available about the FBI's  
15 investigation, both as to the FBI and the defendant, as well  
16 as the ability to intercept and manipulate the transmission  
17 in one second.

18                 THE COURT: Well, I'm sure that if they had  
19 encrypted it and the encryption had to be translated by the  
20 FBI they'd be complaining about the translation of the  
21 encryption. But that's his job, to complain about such  
22 things.

23                 MS. GRATTON: And that would be the government's  
24 view as well. The defendant has a number of tools to  
25 determine that the information gathered and used to identify

1 him is accurate.

2           And when considering whether further disclosure of  
3 how the NIT got to him would significantly alter the quantum  
4 of proof in his favor, the government does think the Court  
5 can look to the confession, look to the full quantum of proof  
6 of evidence available in this case to determine whether some  
7 questioning as to how information was transmitted back  
8 through the operation of the NIT would undermine the fact  
9 that the defendant acknowledged that well before its  
10 execution he was acting as Broden on the Playpen Web site.  
11 So the government does think that that fact is significant  
12 when determining whether the information sought here would  
13 significantly alter the quantum of proof in the defendant's  
14 favor.

15           With respect to the circuit law, I think a review of  
16 the opinions relied on in the *Michaud* case makes clear that  
17 the standard is different there. In the *Munoz* --

18           THE COURT: Well, does that recent decision by the  
19 Fourth Circuit on the question of the transmission tower  
20 impact your argument on that point?

21           MS. GRATTON: I don't believe so, Your Honor. I  
22 don't have that opinion immediately available in front of me;  
23 however, I am aware that the en banc --

24           THE COURT: Well, that opinion came out at the same  
25 time as my opinion came out, so I didn't have the benefit of

1 it when I wrote my opinion.

2 MS. GRATTON: But in that case the Court did  
3 determine that in order to seek those orders, the orders at  
4 issue in those cases for the cell tower information, that the  
5 government was not required to obtain a warrant based on  
6 probable cause.

7 Unfortunately, I don't have the opinion immediately  
8 in front of me. I'd be happy to submit any additional  
9 briefing the Court would like on that question.

10 THE COURT: I'm familiar with it.

11 MS. GRATTON: But in the *Munoz-Walkez* opinion out of  
12 the Ninth Circuit -- or, excuse me, *Hernandez-Meza*, both of  
13 which were cited by the Court in *Michaud* and appear to be the  
14 standard on which the Court made its materiality finding,  
15 describe materiality as a low threshold and said that  
16 anything that would allow a defendant to completely abandon a  
17 planned defense or take a different path is material. Well,  
18 when you compare that to the language in *Caro*, it says,  
19 "Evidence is material if its disclosure would enable him to  
20 significantly alter the quantum of proof in his favor."

21 So reading those two standards side by side, the  
22 government does think that there is a material difference  
23 there that would warrant a ruling that -- especially in light  
24 of the failure to show any issues of irregularity here, in  
25 light of the evidence that has been disclosed and, frankly,

1 the failure to even fully examine the evidence that is  
2 available to him, that at this point the defendant has not  
3 made a showing of materiality sufficient to order any further  
4 disclosure of information related to the delivery of the NIT.

5 Additionally, the government has offered for the  
6 Court's ex parte and in camera consideration a classified  
7 briefing related to the question of privilege. The general  
8 outlines of the issues raised in that filing were included in  
9 the sealed declaration attached as Exhibit 2 to the  
10 government's surreply and made available to the defendant.

11 And it's the government's position, even if the  
12 Court were to find that the defendant has made a threshold  
13 showing of materiality, that the information is nonetheless  
14 privileged. And the question of disclosure is not resolved  
15 simply by the finding of materiality in and of itself,  
16 because we don't get to law enforcement privilege until we've  
17 decided that the information is material and otherwise  
18 subject to disclosure under Rule 16.

19 So if we're there, there has to be some showing  
20 beyond that of a compelling need for the information that  
21 outweighs the public's interest in keeping it private and  
22 secret.

23 THE COURT: Well, the entire case is about the  
24 public's interest in being protected from child pornography,  
25 on the one hand, as against the right of privacy implied by

1 the Fourth Amendment, on the other.

2 MS. GRATTON: As the Court noted in its ruling on  
3 the first and third motions to suppress, that is the balance  
4 that must be struck here. And at least with respect to the  
5 suppression question, the Court found the balance struck in  
6 favor of the public's interest.

7 So the government would ask the Court to consider  
8 the information submitted for the ex parte and in camera  
9 review. Mr. Prabhu, my colleague, is here to address any  
10 further questions in that setting, if the Court has them.

11 And so, even if the defendant has shown materiality,  
12 he has not shown anything beyond that that would indicate a  
13 compelling need for the information sufficient to overcome  
14 the public's interest in keeping it secret, particularly in  
15 light of the fact that we are dealing here with speculative  
16 claims about what could have happened, what might have  
17 happened, without any facts showing that any of that did  
18 happen. The government provided extensive discovery. There  
19 are additional steps that the defendant can take.

20 Thank you, Your Honor.

21 THE COURT: Thank you.

22 MR. GRINDROD: I'll be quick, Your Honor, if I may.

23 THE COURT: You may.

24 MR. GRINDROD: Your Honor, just to address two  
25 points raised by the government, one, with respect to the

1 showing of materiality, the *Caro* case, the Fourth Circuit  
2 case that the government cites, says that, "Evidence is  
3 material as long as there's strong indication that it will  
4 play an important role in uncovering admissible evidence,  
5 aiding in witness preparation, corroborating testimony, or  
6 assisting impeachment or rebuttal."

7 Their argument against materiality is based solely  
8 on Agent Alfin's testimony in court and his declarations, but  
9 there's no way of either corroborating or impeaching that  
10 testimony if we don't have the evidence upon which it's  
11 based. That's what we're asking for.

12 Number two, Your Honor, I know the Court addressed  
13 various positions on materiality, and whoever has it may have  
14 some bias in this case. But I would note that on that  
15 question had we not filed this motion, the government's  
16 position in this litigation was that none of this information  
17 was material and they were not going to produce any of it.  
18 Now they're relying on this other information that they  
19 subsequently produced to say that, this other information  
20 that we want, that we asked for back in March, is not  
21 material.

22 Well, if their first position was none of it's  
23 material, and in their response to our motion they say, okay,  
24 you can have this part of it, and then in their surreply they  
25 say, okay, you can have this part, and now they're saying,

1 well, because we gave you this part, you don't need this  
2 other part you want -- we need it, Your Honor. We need the  
3 evidence. Mr. Matish has a constitutional right to putting  
4 on a defense, and we need the evidence to do so.

5 Thank you.

6 THE COURT: All right. When the Court prepared its  
7 opinion on the defendant's first and third motions to  
8 suppress, the Court ordered that it be filed under seal. At  
9 the time I was preparing that opinion the trial was imminent  
10 in the case, and I did not want the trial of the case to  
11 become a media event, which I thought might affect the  
12 Court's ability to give the defendant a fair trial.

13 Since then, the case has been certified as a complex  
14 case and the case has been postponed. The defendant didn't  
15 ask that it be placed under seal; the Court made that  
16 decision. I don't know whether the defendant believes that  
17 it should be continued under seal at this point in the  
18 proceeding or not.

19 MR. GRINDROD: Your Honor, that's something I've not  
20 really discussed in depth with my client. If it would please  
21 the Court, if I could have a day or until later this  
22 afternoon to notify the Court of our position on that --

23 THE COURT: I don't know. I mean, I -- you know,  
24 sometimes when cases involve a difficult or controversial  
25 issue, which this case certainly does, they change the case

1 to somebody against John Doe, or something like that, because  
2 somebody doesn't want their name forever associated with a  
3 case, regardless of the outcome, when it involves a sensitive  
4 topic like child pornography.

5 So I don't know what to tell you about that. All I  
6 can say is if the defendant wants the opinion under seal,  
7 I'll certainly consider that.

8 MR. GRINDROD: I appreciate it, Your Honor. I'll  
9 make a filing of some sort one way or the other, if it  
10 pleases the Court.

11 THE COURT: But I need for you to do that quite  
12 soon.

13 MR. GRINDROD: Yes, Your Honor, understood.

14 THE COURT: All right. Well, having initially  
15 placed its opinion under seal, and not having an answer as to  
16 whether the defendant wants it to remain so, I will not go  
17 into the Court's thinking at this time. I'll prepare a  
18 written opinion, which I would do anyway, but I'll hold off  
19 on publishing any opinion until I hear from the defendant on  
20 that issue.

21 Do you think you can let me know --

22 MR. GRINDROD: This afternoon, Your Honor.

23 THE COURT: Okay. All right.

24 Is there anything further from either side, then?

25 MS. GRATTON: No, Your Honor.

1                   MR. GRINDROD: Nothing from the defense, Your Honor.

2                   THE COURT: All right. Are there any remaining  
3 pretrial motions pending, other than this discovery motion?

4                   MS. GRATTON: No, Your Honor.

5                   THE COURT: All right. Well, I mean, some of the  
6 discovery has been handled by agreement between the parties,  
7 and the Court is really not privy to all that.

8                   MR. GRINDROD: Correct, Your Honor.

9                   MS. GRATTON: Yes, Your Honor.

10                  THE COURT: So as far as I know, this is the only  
11 motion that the Court hasn't decided.

12                  MR. GRINDROD: I think that's right, Your Honor.

13                  MS. GRATTON: That's correct, Your Honor.

14                  THE COURT: All right. Well, I'll wait to hear from  
15 you, then, Mr. Grindrod.

16                  I don't think it's necessary, regardless of the  
17 Court's decision, to have an in camera hearing. I've been  
18 supplied with the government's brief that was marked  
19 "Secret," which I have reviewed, and I think that the  
20 materials that I reviewed in preparation for this hearing  
21 would enable the Court to make a decision on whether the  
22 privilege would apply if the Court finds the evidence  
23 material without the necessity of an in camera hearing.

24                  (The hearing adjourned at 1:35 p.m.)

25

## CERTIFICATION

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/ s

Heidi L. Jeffreys

June 16, 2016

Date

Heidi L. Jeffreys, Official Court Reporter